

U.S. Department of Transportation

Federal Aviation Administration

Interface Control Document

NAS Infrastructure Management System Manager/
Managed Subsystem
using the
Simple Network Management Protocol Version 1(SNMPv1)

INTERFACE CONTROL DOCUMENT

APPROVAL SIGNATURE PAGE

NAS Infrastructure Management System (NIMS) Manager/
Managed Subsystem
using the
Simple Network Management Protocol Version 1(SNMPv1)

APPROVAL SIGNATURES

PARTICIPANT	NAME	DATE
NIMS Product Team	Michael Shveda	

REVISION RECORD			
REVISION LETTER	DESCRIPTION	DATE	ENTERED BY
- -	Initial Release	22 July 97	
A	Incorporation of reviewer comments	01 May 98	

TABLE OF CONTENTS

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
1. SCOPE		1
1.1	Scope	1
1.1	Subsystem responsibility list	1
1.2	1
2. APPLICABLE DOCUMENTS		2
2.1	Government documents	2
2.2	Non-government documents	2
2.3	Document sources	4
2.3.1	FAA documents	4
2.3.2	IETF documents	4
2.3.3	ISO documents	4
3. INTERFACE REQUIREMENTS		5
3.1	General requirements	5
3.2	Functional requirements	5
3.2.1	Application process	6
3.2.1.1	Identification of application process	6
3.2.1.2	Type of services required by the AP	7
3.2.1.2.1	Event reporting	7
3.2.1.2.2	Solicited data reporting	8
3.2.1.2.3	Control	8
3.2.1.2.3.1	Initiate action	8
3.2.1.2.3.2	Modify management information	9
3.2.1.3	Information units	9
3.2.1.3.1	Information code	9
3.2.1.3.1.1	Protocol data unit	10
3.2.1.3.2	Information structure	10
3.2.1.3.2.1	NIMS MIB structure	11
3.2.1.3.2.2	NIMS Standard Traps	18
3.2.1.3.2.2.1	Operating Status Change	18
3.2.1.3.2.3	Managed subsystem specific Traps	18
3.2.1.3.2.3.1	Availability Status Change	19
3.2.1.3.2.3.2	Configuration Change	19
3.2.1.3.2.3.3	Performance Threshold Transition	19
3.2.1.3.2.3.4	Security Violation	20
3.2.1.3.2.3.5	Shut Down Complete	20
3.2.1.3.3	Information unit segmentation	20
3.2.1.3.4	Information flow	20
3.2.1.3.5	Frequency of transmission	21

TABLE OF CONTENTS (Continued)

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
3.2.1.4	Interface summary table	21
3.2.1.5	Quality of service.....	21
3.2.1.5.1	Information priority	21
3.2.1.5.2	Information security	21
3.2.1.6	Error handling.....	21
3.2.2	Communication requirements.....	23
3.2.2.1	Application layer	23
3.2.2.2	Presentation layer	23
3.2.2.3	Session layer	23
3.2.2.4	Transport layer.....	23
3.2.2.5	Network layer	23
3.2.2.6	Addressing	23
3.2.2.7	Subnetwork profile 1: point-to-point interface.....	24
3.2.2.7.1	Dedicated connection	25
3.2.2.7.2	Dial-up connection	25
3.2.2.8	Subnetwork profile 2: local area network interface.....	26
3.2.2.9	Subnetwork profile 3: packet switching interface	26
3.3	Security	26
4.	QUALITY ASSURANCE PROVISIONS	27
4.1	General.....	27
4.2	Special verification levels and methods	27
4.3	Verification levels and methods	27
4.4	Quality conformance inspections	27
4.5	Verification requirements	28
4.6	Verification methods	28
5.	PREPARATION FOR DELIVERY.....	33
6.	NOTES.....	34
6.1	Operational concept.....	34
6.1.1	NAS Infrastructure Management (NIM) operational concept.....	34
6.1.1.1	NIM element mission requirements	34
6.1.1.1.1	NIMS sub-element mission requirements	34
6.1.1.1.2	National Operations Control Center (NOCC)	34
6.1.1.1.3	Operations Control Center (OCC).....	35
6.1.1.1.4	Work Center (WC)	35
6.2	Definitions	35
6.3	Abbreviations and acronyms	36

TABLE OF CONTENTS (Continued)

<u>Paragraph</u>	<u>Title</u>	<u>Page</u>
APPENDIX A SMI Definitions Of SNMPV1 Constructs For FAA NIMS.....A-1		
A.1	FAA NIMS MIB.....	A-1
A-2	NIMS-Standard Traps.....	A-4
A-2.1	opStatusChange Trap.....	A-4

LIST OF FIGURES

FIGURE 3-1. NIMS FUNCTIONAL CONNECTIVITY.....	5
FIGURE 3-2. NIMS MANAGER/AGENT INTERFACE.....	6

LIST OF TABLES

TABLE 3-1. COMMON RESOURCES GROUP.....	15
TABLE 3-2. COMMON RESOURCES GROUP ATTRIBUTE TABLE (EXAMPLE).....	16
TABLE 3-3. SPECIFIC RESOURCES GROUP ATTRIBUTE TABLES (EXAMPLE).....	17
TABLE 4-1. VERIFICATION REQUIREMENTS TRACEABILITY MATRIX	29
TABLE 4-1. VERIFICATION REQUIREMENTS TRACEABILITY MATRIX (CONT.).....	30
TABLE 4-1. VERIFICATION REQUIREMENTS TRACEABILITY MATRIX (CONT.).....	31
TABLE 4-1. VERIFICATION REQUIREMENTS TRACEABILITY MATRIX (CONT.).....	32

1. SCOPE

1.1 Scope

This Interface Control Document (ICD) is prepared in accordance with FAA-STD-025d. It provides interface requirements to enable the Federal Aviation Administration (FAA) National Airspace System Infrastructure Management System (NIMS) Managers to remotely monitor and control Managed Subsystems (i.e., NAS Subsystem managed by the NIMS Manager). The NIMS Manager will manage the NAS Subsystems by sending management operation requests to and receiving notifications from the NIMS Agents within the NAS Subsystems. Therefore, this ICD specifies interface requirements between the NIMS Manager and the NIMS Agent (See Figure 3.1). The interface between the NIMS Agent and the NAS subsystem is not the subject of this ICD.

This ICD provides Simple Network Management Protocol Version 1 (SNMPv1) protocol requirements necessary for satisfying requirements specified in the NIMS Manager/Managed Subsystem IRD, NAS-IR-51070000. In addition, this ICD specifies a set of managed objects, a subset of which is defined. Managed objects referenced in this ICD but not defined should be defined in the subsystem-specific ICD.

Non-developmental interfaces, which provide the required functional capability in a different manner than specified in this ICD, may be used upon agreement by the NAS Subsystem Integrated Product Team (IPT) and the NIMS Product Team (PT). If a functional capability required in this document is not available, a viable alternative may be provided, once agreed to by the NAS Subsystem IPT and the NIMS PT. [NOTE: The security requirements provided or referenced in this document are not complete and will be finalized upon completion of security guidance and policy being developed by the NIMS Security Working Group.]

This generic NIMS ICD will enable the development of specific NAS Subsystem ICDs which would be approved by the NAS Subsystem IPT and the NIMS PT. The specific ICD should not duplicate the requirements in the generic ICD, but only provide unique NAS Subsystem requirements and notification of waived NIMS requirements. The specific ICD will be incorporated as an appendix to the NIMS ICD.

1.2 Subsystem responsibility list

Subsystem/Equipment	Common Name	Responsible Organization
NIMS Manager	NIMS Manager	Infrastructure IPT/NIMS PT
NAS Subsystem	NIMS Agent	NAS Subsystem IPT

2. APPLICABLE DOCUMENTS

The following documents form a part of this ICD to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this ICD, the contents of this ICD shall be the superseding requirements.

2.1 Government documents

Federal Aviation Administration Specifications

ENET1370-001.1:1995	FAA Enterprise Network Naming and Addressing Standard
FAA-E-2911:1998	System Level Specification for NAS Infrastructure Management System (NIMS) Managed Subsystems
FAA-E-2912:1998	System Level Specification for NAS Infrastructure Management System (NIMS)

Federal Aviation Administration Standards

FAA-HDBK-002:1996	Open Systems Management Handbook
FAA-STD-025d:1995	Preparation of Interface Documentation
FAA-STD-039b:1996	Open Systems Architecture and Protocols
FAA-STD-043a:1994	NAS Open Systems Interconnection Priority
FAA-STD-045:1994	Open Systems Security Standard Protocols and Mechanisms

Other FAA Documents

NAS-IC-43020001:1996	NADIN PSN X.25 Packet Mode Users Interface Control Document
NAS-IR-40010001:1995	NAS LAN Users Systems Interface Requirements Document

2.2 Non-government documents

Electronic Industries Association (EIA)

EIA/TIA-232E:1991	Interface Between Data Terminal Equipment and Data Circuit -Terminating Equipment Employing Serial Binary Data Interchange
EIA-530: 1987	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Termination Equipment

Internet Engineering Task Force, Request for Comment

IETF RFC 768:1980	User Datagram Protocol (UDP)
IETF RFC 791:1981	Darpa Internet Program Protocol Specification - Internet Protocol
IETF RFC 792:1981	Internet Control Message Protocol
IETF RFC 959:1985	File Transfer Protocol (FTP)
IETF RFC 1042:1988	Standard for the Transmission of IP Datagrams over IEEE 802 Networks
IETF RFC 1155:1990	Structure and Identification of Management Information for TCP/IP-based Internets
IETF RFC 1157:1990	A Simple Network Management Protocol (SNMP)
IETF RFC 1212:1991	Concise MIB Definitions
IETF RFC 1213:1991	Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II
IETF RFC 1215:1991	A Convention for Defining Traps for use with the SNMP
IETF RFC 1332: 1992	The PPP Internet Protocol Control Protocol (IPCP)
IETF RFC 1381:1992	SNMP MIB Extension for X.25 LAPB
IETF RFC 1382:1992	SNMP MIB Extension for the X.25 Packet Layer
IETF RFC 1471:1993	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
IETF RFC 1473:1993	The Definitions of Managed Objects for IP Network Control Protocol of the Point-to-Point Protocol

IETF RFC 1512:1993	FDDI Management Information Base
IETF RFC 1643:1994	Definition of Managed Objects for the Ethernet-like Interfaces Types
IETF RFC 1661:1994	The Point-to-Point Protocol (PPP)

International Organization for Standardization (ISO)

ISO 2110:1989	Information Technology - Data Communication - 25-Pole DTE/DCE Interface Connector and Contact Number Assignments
ISO 8824:1987	Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)
ISO 8825:1987	Information Processing Systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)
ISO 9542:1988	Information Technology - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service

2.3 Document sources

2.3.1 FAA documents

Copies of FAA specifications, standards, and publications may be obtained from the Contracting Officer, Federal Aviation Administration, 800 Independence Avenue, S.W., Washington, D.C., 20591. Requests should clearly identify the desired material by number and date, and state the intended use of the material.

2.3.2 IETF documents

Copies of IETF standards may be obtained from electronically from the world wide web @ http://www.aetc.af.mil/rfc_main_index.html.

2.3.3 ISO documents

Copies of ISO standards may be obtained from the American National Standards Institute, 11 West 42nd Street, New York, NY, 10036.

3. INTERFACE REQUIREMENTS

3.1 General requirements

This ICD describes the interface requirements between the NAS Infrastructure Management System (NIMS) Manager and NIMS Agents of the managed subsystem. The agent may be an embedded agent, proxy agent, or proxy agent/concentrator.

- a) The connectivity between the NIMS Manager and the NIMS Agent shall enable NIMS to monitor and control NAS Subsystems as shown in Figure 3-1. [NOTE: Connectivity between the NIMS Manager and NIMS Agent may include point-to-point, local area networks (LAN), and/or wide area networks (WAN).]
- b) Proxy agents shall be used to allow NAS subsystems, using proprietary and non-standard management functions, to communicate with the NIMS Manager.

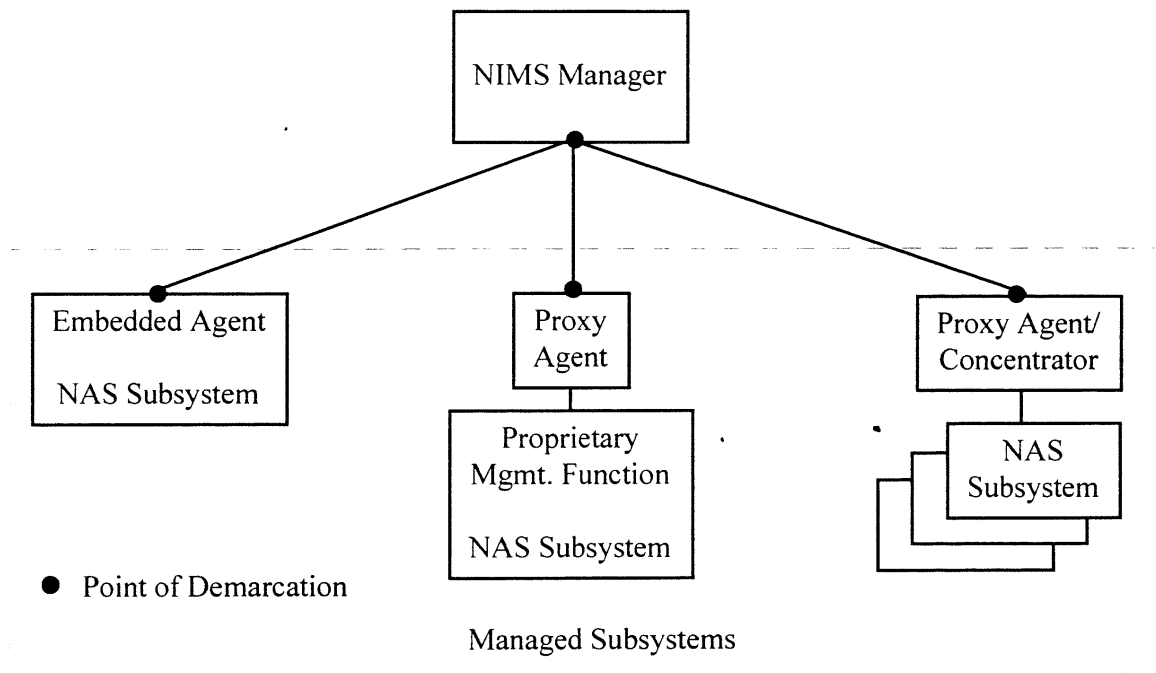
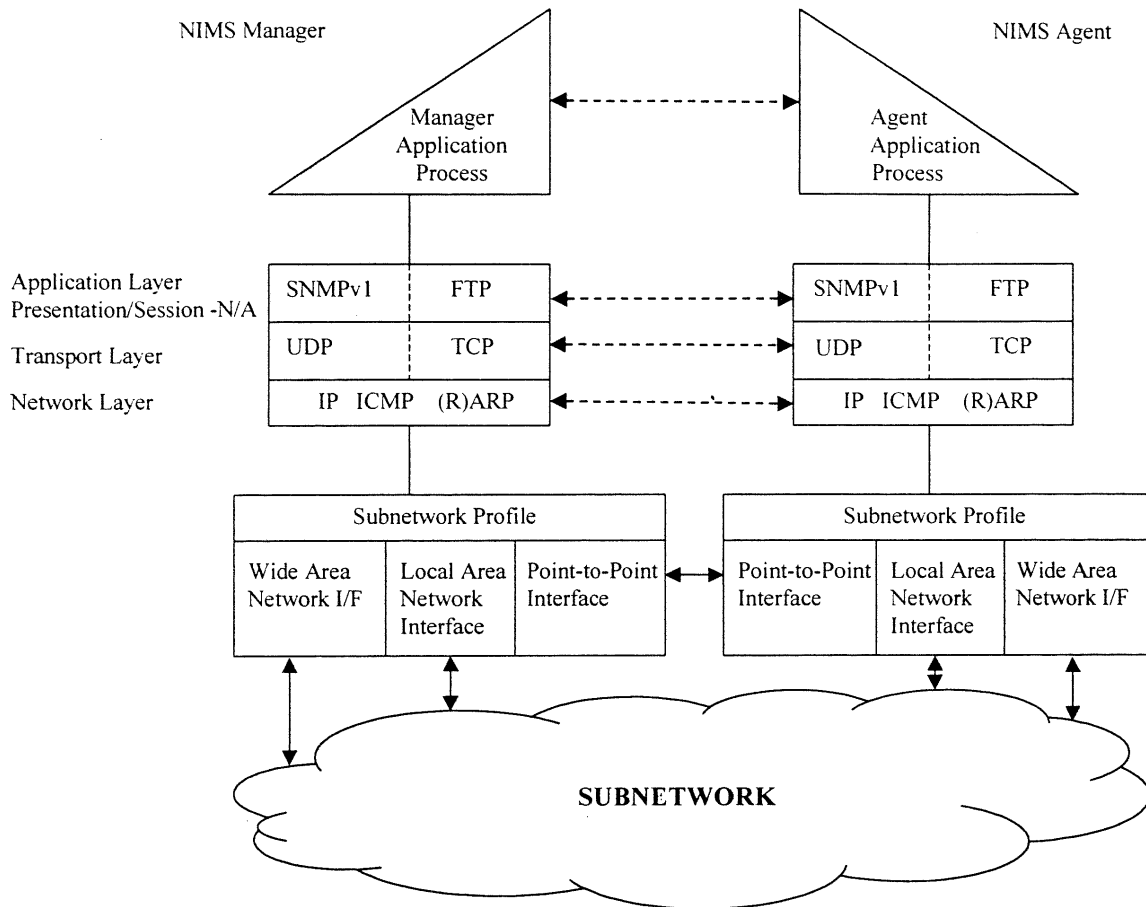


Figure 3-1. NIMS Functional Connectivity

3.2 Functional requirements

- a) The functional interface between the NIMS Manager and the NIMS Agent shall use the 5-layer Internet Protocol Suite (IPS) which provides peer-to-peer communication as illustrated in Figure 3-2.
- b) The functional interface shall be implemented in accordance with requirements provided in this section.



ACRONYMS

(R)ARP	(Reverse) Address Resolution Protocol
FTP	File Transfer Protocol
ICMP	Internet Control Management Protocol
IP	Internet Protocol
N/A	not applicable
SNMPv1	Simple Network Management Protocol Version 1
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Figure 3-2. NIMS Manager/Agent Interface

3.2.1 Application process

3.2.1.1 Identification of application process

- The application which implements manager monitor and control requirements specified in the System Requirements System Level Specification (SLS) for NAS Infrastructure Management System (NIMS), FAA-E-2912, shall be identified as the NIMS Manager application process (AP).

- b) The application which implements the applicable monitor and control requirements specified in the System Level Specification (SLS) for NAS Infrastructure Management System (NIMS) Managed Subsystems, FAA-E-2911, shall be identified as the NIMS Agent AP.

3.2.1.2 Type of services required by the AP

- a) Reliable event reporting, solicited data reporting, and control services shall be provided by one or a combination of the following:
- system design
 - reliable communications subnetwork(s)
 - supplemental polling of trappable resource attributes
 - retransmission of messages

3.2.1.2.1 Event reporting

- a) The NIMS Agent shall send an SNMP Trap to the NIMS Manager upon occurrence of an event.
- b) The NIMS Manager and NIMS Agent shall support the following events:
- Operating Status Change
 - Administrative State Change
 - Availability Status Change
 - Configuration Change
 - Performance Threshold Transition
 - Access Control Rule Violation
 - Completion of Requested Action
- c) When the reliability of event reporting is of concern, the NIMS Manager shall periodically poll the NIMS Agent, with SNMP GetRequest messages, to retrieve the managed resource attribute(s) associated with the reportable events.
- d) In conformance with SNMPv1, the NIMS Agent shall respond to each poll by sending an SNMP GetResponse message to the NIMS Manager specifying the current value of the requested managed resource attribute(s).
- e) The invocation and frequency of polling for event occurrences shall be operationally determined.

3.2.1.2.2 Solicited data reporting

- a) The NIMS Manager shall be able to request the value(s) of a resource attribute(s) by sending the following SNMP message types to the NIMS Agent:
 - GetRequest
 - GetNextRequest
- b) Type of resource attributes request shall include the following:
 - Monitored attributes
 - Control attributes
- c) The NIMS Agent shall confirm the request by sending an SNMP GetResponse containing the requested resource attribute value(s) or the appropriate SNMP error-status to indicate the reason for not satisfying the request.
- d) The NIMS Manager shall be able to retrieve the security log data from the Managed Subsystem using the File Transfer Protocol (FTP).

3.2.1.2.3 Control

3.2.1.2.3.1 Initiate action

- a) The NIMS Manager shall initiate actions by sending an SNMP SetRequest to the NIMS Agent.
- b) The NIMS Manager and NIMS Agent shall support the following types of actions:
 - Reset subsystem
 - Perform diagnostics
 - Set administrative state
- c) The NIMS Agent shall confirm the invocation of the action by returning a GetResponse containing the value(s) of the attribute(s) contained in the invoking SetRequest.
- d) The NIMS Manager and the NIMS Agent shall use standard SNMP protocol data units to exchange managed resource attributes for the purposes of determining the status of the invoked action.

3.2.1.2.3.2 Modify management information

- a) The NIMS Manager shall be able to change, add, or delete managed resource attributes by sending an SNMP SetRequest to the NIMS Agent.
- b) Managed resources which may be modified shall include the following:
 - Fault management (i.e. operating status) thresholds
 - Automatic fault isolation parameters
 - Fault recovery processing parameters
 - Event forwarding discriminators
 - Configuration attributes
 - Performance thresholds
 - Access control rules
- c) In conformance to SNMPv1, the NIMS Agent shall send an SNMP GetResponse message to the NIMS Manager containing the value(s) of the modified attribute(s) or the appropriate SNMP error-status to indicate the reason for not satisfying the request.

3.2.1.3 Information units

- a) Management information shall be exchanged between the NIMS Manager and NIMS Agent using messages formatted in accordance with SNMPv1.
- b) Security logs shall be transferred from the NIMS Agent to the NIMS Manager using files formatted in accordance with FTP.

3.2.1.3.1 Information code

- a) The management information shall be defined using a subset of the Abstract Syntax Notation One (ASN.1): ISO 8824 in accordance with RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets, with one exception. The use of zero as an enumeration value in enumerated Integer types, which is prohibited by RFC 1155, is not prohibited in the definition of management information specific to the particular managed subsystem type.
- b) Management information shall be encoded, for data transfer, using Basic Encoding Rules (BER) in accordance with ISO 8825.

3.2.1.3.1.1 Protocol data unit

- a) The following SNMPv1 protocol data units (PDU) shall be used to exchange management information between the NIMS Manager and the NIMS Agent:
- GetRequest
 - GetNextRequest
 - SetRequest
 - GetResponse
 - Trap

3.2.1.3.2 Information structure

- a) The NIMS Manager and NIMS Agent shall support the MIB II structure defined in RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets and illustrated in Figure 3-3. The object identifier for MIB II is 1.3.6.1.2.1.
- b) The provided MIB II implementation shall be supplemented by the private MIB extensions, including the FAA MIB.
- c) The following MIB II object groups shall be supported to manage the interface between the NIMS Manager and the NIMS Agent (see Figure 3-3):
- system
 - interfaces
 - ip
 - icmp
 - udp
 - transmission
 - snmp
- d) When required, the following transmission group MIBs shall be supported (see Figure 3-3):
- RFC-1643: ISO 8802-3 CSMA/CD MIB
 - RFC 1512: FDDI MIB
 - RFC 1382: X.25 Packet Layer MIB
 - RFC 1381: X.25 LAPB MIB**
 - RFC 1471: Point-to-Point Link Control Protocol MIB
 - RFC 1473: Point-to-Point Network Control Protocol MIB
- (e) MIB objects shall be named in accordance with RFC 1157.

```
.1 iso
  .3 org
    .6 dod
      .1 internet
        .2 mgmt
          .1 mib-II (1.3.6.1.2.1)
            .1 system
            .2 interfaces
            .4 ip
            .5 icmp
            .7 udp
            .10 transmission
              .5 x25lapb
              .7 csma/cd
              .15 fddi
              .16 x25Packet
              .23 point-to-point
                .1 ppp-lcp
                .3 ppp-ncp
            .11 snmp
```

Figure 3-3. MIB-II Structure

3.2.1.3.2.1 NIMS MIB structure

- a) The NIMS Manager and NIMS Agent shall support the NIMS MIB structure defined in Appendix A, Section A.1 and illustrated in Figure 3-4 and 3-5.
- b) The object identifier (OID) name, “nims”, shall be used to reference the NIMS FAA Enterprise MIB.
- c) The OID number, “1.3.6.1.4.1.2120.1”, shall be used to reference the NIMS FAA Enterprise MIB.
- d) The NIMS MIB shall be defined in accordance with RFC 1212 and Table 3-1 and include the following MIB groups:
 - Common Resources Group (CRG) - Common MIB consisting of standard resource attributes for all managed resources (i.e., subsystems, subsystem functions, agent functions, hardware components, software components, external interfaces, etc.). See Table 3-1 and Table 3-2. The CRG OID is {nims 1}.

```

.1 iso
.3 org
.6 dod
.1 internet
.2 mgmt
.1 mib-II (1.3.6.1.2.1)
.4 private
.1 enterprise
.2120 faaEnterprise (1.3.6.1.4.1.2120)
.1 nims (1.3.6.4.1.2120.1)
.1 commonResourcesGroup
.1 crgNumber
.2 crgTable
.1 crgEntry
.1 crgID (Table Index)
.2 crgDescr
.3 crgType
.4 crgOpStatus
.5 crgAdminState
.6 crgOpTime
.7 crgSrgOID
.2 specificResourcesGroup
.1 group-name-1ResourcesGroup
.2 group-name-2ResourcesGroup
.
.
.
.n group-name-nResourcesGroup
.1 group-name-n.1Number
.2 group-name-n.1Table
.1 group-name-n.1Entry
.1 group-name-n.1ID (Table Index)
.2 group-name-n.1-attribute
.3 group-name-n.1-attribute
.
.
.
.n group-name-n.1-attribute
.3 group-name-n.2Number
.4 group-name-n.2Table
.1 group-name-n.2Entry
.1 group-name-n.2ID (Table Index)
.2 group-name-n.2-attribute
.3 group-name-n.2-attribute
.
.
.
.n group-name-n.2-attribute
.5 group-name-n.3Number
.6 group-number.3Table
.etc

```

Figure 3-4. Example - NIMS MIB Structure

```

1.3.6.1.4.1 enterprise
.2120 faaEnterprise
.1 nims
.1 commonResourcesGroup
.1 crgNumber
.2 crgTable
.1 crgEntry
.1 crgID
.2 crgDescr
.3 crgType
.4 crgOpSta
.5 crgAdminState
.6 crgOpTime
.7 crgSrgOID
.2 specificResourcesGroup
.37 wmscrResourcesGroup
.1 wmscrSubsystemNumber
.2 wmscrSubsystemTable
.1 wmscrEntry
.1 wmscrID
.2 wmscrAttributeName
.3 wmscrAttributeName
.4 wmscrAttributeName
.5 wmscrAttributeName
.6 wmscrAttributeName
.3 wmscrSubFunctionNumber
.4 wmscrSubFunctionTable
.1 wmscrSubFunctionEntry
.1 wmscrSubFunctionID
.2 wmscrSubFunctionAttributeName
.3 wmscrSubFunctionAttributeName
.5 wmscrAgentFunctionNumber
.6 wmscrAgentFunctionTable
.1 wmscrAgentFunctionEntry
.1 wmscrAgentFunctionID
.2 wmscrAgentFunctionAttributeName
.3 wmscrAgentFunctionAttributeName
.4 wmscrAgentFunctionAttributeName
.53 hvacResourcesGroup
.1 hvacSubsystemNumber
.2 hvacSubsystemTable
.1 hvacEntry
.1 hvacID
.2 hvacAttributeName
.3 hvacAttributeName
.4 hvacAttributeName
.5 hvacAttributeName
.6 hvacAttributeName
.3 hvacAgentFunctionNumber
.4 hvacAgentFunctionTable
.1 hvacAgentFunctionEntry
.1 hvacAgentFunctionID
.2 hvacAgentFunctionAttributeName
.3 hvacAgentFunctionAttributeName
.4 hvacAgentFunctionAttributeName

```

Figure 3-5. Example - NIMS Agent MIB

- Specific Resources Group (SRG) - Group of MIBs, each MIB consisting of resource attributes for the specific NAS subsystem type (i.e., WMSCR, ASR) or model (i.e., DME). See Table 3-3. The SRG OID is {nims 2}.
- e) SRGs for NAS Subsystems shall be assigned a subarc under the SRG arc by the NIMS PT.
- f) The Common Resources Group shall provide the following information about the managed resource in accordance with Table 3-1:
- Resource identifier
 - Description
 - Type
 - Operating status
 - Administrative state
 - Time entered in current operating state
 - Specific Resources Group Object Identifier
- g) The Specific Resources Group shall include (but not be limited to) availability status information about the managed resource, subject to the managed resource's ability to detect and report such information. The availability status information to be reported shall include (but not be limited to) the following conditions of the managed resource:
- Power on/off
 - Online/offline
 - In maintenance
 - Hot/cold standby
- h) Each managed resource shall be assigned a unique resource identifier by the FAA naming authority for identifying the resource and the associated attributes.
- i) An agent managing multiple NAS subsystems shall support the SRG MIB for each NAS subsystem.
- j) The agent shall, at a minimum, maintain managed resources and attributes for the NAS subsystems being monitored.

Table 3-1. Common Resources Group

Object	Syntax	Access	Status	Description
crgNumber OID::={commonResources Group 1}	INTEGER	RO	Mandatory	Number of Entries in crgTable
crgTable OID::={commonResources Group 2}	SEQUENCE OF CrgEntry	NA	Mandatory	Table of common managed resource attributes
crgEntry OID::={crgTable 1}	CrgEntry	NA	Mandatory	Status attributes for particular NIMS Agent component {crgID, crgDescr, crgType, crgOpSta, crgAdminState, crgOpTime}
crgID OID::={crgEntry 1}	Display String (Size [0..20])	RO	Mandatory	Unique printable ASCII identifier associated with the specific managed resource component
crgDescr OID::={crgEntry 2}	Display String (Size [0..50])	RO	Mandatory	Information about the managed resource component
crgType OID::={crgEntry 3}	INTEGER {subsystem (1), subFunction (2), hwComponent (3), swComponent (4), extInterface (5), agentFunction (6)}	RO	Mandatory	Type of managed resource component – subsystem (1), subsystem function (2), hardware component (3), software component (4), external subsystem interface (5), agent function (6)
crgOpStatus OID::={crgEntry 4}	INTEGER {normal (1), warning (2), degraded (3), failed (4)}	RO	Mandatory	Operating status of managed resource component - (1) normal, (2) warning, (3) degraded, (4) failed
crgAdminState OID::={crgEntry 5}	INTEGER {locked (1), unlocked (2), shutting down (3)}	RW	Mandatory	Administrative state of managed resource component - (1) locked, (2) unlocked, (3) shutting down Note 1: If the resource cannot have its Administrative State changed remotely, the Administrative State will be permanently set to “unlocked”, and when a Set-Request is received to SET the value to “locked” or “shuttingDown”, the resultant Get- Response shall be returned with a value of “unlocked”. Note 2: If the resource does support the shuttingDown state, the resource shall generate a managed subsystem-specific trap whenever the value of the Administrative State transitions from “shuttingDown” to “locked”.

				Note 3: If the resource does not support the "shutting down" state, when a Set-Request is received to SET the value to "shutting down", the resource shall immediately transition to "locked" and the resultant Get-Response shall be returned with a value of "locked".
crgOpTime OID::={crgEntry 6}	TimeTicks	RO	Mandatory	The value of sysUpTime when the managed resource entered its current status or state
crgSrgOID OID::={crgEntry 7}	Object Identifier	RO	Mandatory	OID of the Specific Resources Group table that contains additional management information about this resource

Table 3-2. Common Resources Group Attribute Table (Example)

CrgID	crgDescr	crgType	CrgOpStatus	crgAdminState	crpOpTime	crgSrgOID	crgAvailStatus
<ZLC.WMSCR.1.0>	WMSCR_ZLC subsystem	1	1	2	1/23/87:00:00:00	wmscrSubsystemTable	2
<ZLC.WMSCR.1.1>	WMSCR_ZLC subsystem function	2	1	2	1/23/87:00:00:00	wmscrSubFunctionTable	2
<ZLC.WMSCR.1.2>	WMSCR_ZLC h/w component	3	1	2	1/23/87:00:00:00	wmscrHwComponentTable	2
<ZLC.WMSCR.1.3>	WMSCR_ZLC s/w component	4	1	2	1/23/87:00:00:00	wmscrSwComponentTable	2
<ZLC.WMSCR.1.4>	WMSCR_ZLC external interface	5	4	1	1/23/87:00:00:00	wmscrExtInterfaceTable	1
<ZLC.WMSCR.1.5>	WMSCR_ZLC agent function	6	1	2	1/23/87:00:00:00	wmscrAgentFunctionTable	2

Note: <> represents an example display-string-oriented index into the crgTable, where (in this example) the first element of the index ("ZLC") represents the location, the second element ("WMSCR") is the subsystem type, the third element ("1") is an identifier of the instance of that subsystem type at that location (i.e., WMSCR #1 at ZLC), and the fourth element is an arbitrary integer that makes each subelement of the subsystem unique. Note that this is only an example index – the syntax of the indices that will be actually used will be defined in the context of the specific management domain to which the subsystem will belong.

Table 3-3. Specific Resources Group Attribute Tables (Example)

Table X-1. wmscrSubsystem Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.0>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.2.0>	<value>	<value>	<value>	<value>	<value>

Table X-2. wmscrSubFunction Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.1>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.2.1>	<value>	<value>	<value>	<value>	<value>

Table X-3. wmscrHwComponent Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.2>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.2.2>	<value>	<value>	<value>	<value>	<value>

Table X-4. wmscrSwComponent Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.3>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.2.3>	<value>	<value>	<value>	<value>	<value>

Table X-5. wmscrExInterface Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.4>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.1.4>	<value>	<value>	<value>	<value>	<value>

Table X-6. wmscrAgentFunction Table

WMSCR Ids	Attribute-1	Attribute-2	Attribute-3	Attribute-...	Attribute-n
<ZLC.WMSCR.1.5>	<value>	<value>	<value>	<value>	<value>
<ZLC.WMSCR.2.5>	<value>	<value>	<value>	<value>	<value>

Note: These subtables correspond to the Specific Resources Group tables for WMSCR called out in the example Common Resources Group Attribute table illustrated in Table 3-2. These tables are for illustrative purposes only, and are not representative (except in the most general way) of the tables that will actually be used to contain WMSCR.

3.2.1.3.2.2 NIMS Standard Traps

NIMS Standard Traps shall be implemented in accordance with RFC 1215, "A Convention for Defining Traps for Use with SNMP" and include, but not be limited to, Traps for changes in Operating Status.

3.2.1.3.2.2.1 Operating Status Change

- a) The NIMS Agent shall notify the NIMS Manager of a change in the operating status of a managed resource by sending opStatusChange Trap, in accordance with Appendix A, Section A.2.1.
- b) The opStatusChange Trap shall include the SNMP object name (crgOpStatus) and current value of crgOpStatus: NORMAL (encoded as 1), which indicates that resource is operating in the ideal operating range; WARNING (encoded as 2), which indicates that the resource is still capable of performing all of its functions at the ideal level of performance, but some aspect of the resource has changed such that management action is required;¹ DEGRADED (encoded as 3), which indicates that the resource is not operating in the ideal operating range but operating within an acceptable operating range; and FAILED (encoded as 4), which indicates that the resource is operating outside the acceptable operating range.

3.2.1.3.2.3 Managed subsystem specific Traps

- a) Managed subsystem specific Traps shall be implemented in accordance with RFC 1215, "A Convention for Defining Traps for Use with SNMP" and include, but not limited to, Traps for the following events:
 - Availability Status Change
 - Configuration Change
 - Performance Threshold Transition
 - Access Control Rule Violation
 - Shut Down Complete
- b) For each resource that has one or more resource-specific Traps defined for it, all such Traps shall be defined using the object identifier of the specific resource group subtree for that resource in the ENTERPRISE clause of the trap definition.

¹ For example, a resource with one or more internal redundant components could transition from "normal" to "warning" when the last redundant component has failed, leaving the only a single component operating.

3.2.1.3.2.3.1 Availability Status Change

- a) For each managed resource required to notify the NIMS Manager upon change of availability status, the NIMS Agent shall notify the NIMS Manager of changes in the availability status of a managed resource by sending one or more availability status change Traps.
- b) The information conveyed in the availability status change Trap(s) shall indicate the current availability status immediately following a change in status. The availability status values may include, but not be limited to, transitions between the following conditions: (1) Online/offline; (2) poweron/poweroff; (3) in or out of maintenance; and (4) hot/cold standby.

3.2.1.3.2.3.2 Configuration Change

- a) For each attribute of the managed resource required to notify the NIMS Manager upon change of attribute value, the NIMS Agent shall notify the NIMS Manager of a change in a configuration attribute by sending a Configuration Change Trap.
- b) A unique name shall be defined for each configuration attribute.
- c) A unique Configuration Change Trap shall be defined for each configuration attribute requiring notification upon change in value.
- d) Each Configuration Change Trap shall include the SNMP object name and current value of the attribute being reported.

3.2.1.3.2.3.3 Performance Threshold Transition

- a) For each attribute designated as a performance threshold for which transitions across the threshold are to be notified to the NIMS Manager, the NIMS Agent shall notify the NIMS Manager when the value of a performance attribute transitions across the threshold by sending a Performance Threshold.
- b) A unique name shall be defined for each performance threshold attribute.

- c) A unique Performance Threshold Change Trap shall be defined for each performance threshold attribute.
- d) Each Performance Threshold trap shall include the SNMP object name and current value of the attribute being reported.

3.2.1.3.2.3.4 Security Violation

- a) For each attribute designated as a security violation indicator to be notified to the NIMS Manager, the NIMS Agent shall notify the NIMS Manager when a security violation has occurred by sending Security Violation Trap.
- b) A unique name shall be defined for each security violation attribute.
- c) A unique Security Violation Trap shall be defined for each security violation attribute.
- d) Each Security Violation Trap shall include the SNMP object name and value of the security violation attribute.

3.2.1.3.2.3.5 Shut Down Complete

- a) For each managed subsystem that supports the Shutting Down value of the Administrative State, the NIMS Agent shall notify the NIMS Manager when the value of the Administrative State transitions from "ShuttingDown" to "Locked".
- b) Each Trap indicating the completion of Shut Down shall include the name and resultant value (i.e., "Locked") of the Administrative State attribute.

3.2.1.3.3 Information unit segmentation

- a) The maximum message size shall be at least 484 characters.

3.2.1.3.4 Information flow

- a) The information flow shall be as described in Table 3-4.
- b) Event reports shall be provided by the NIMS Agent.
- c) The request for management data shall be provided by the NIMS Manager.
- d) Solicited management data shall be provided by the NIMS Agent.

- e) Control operations shall be initiated by the NIMS Manager.
- f) Confirmation or the completion of control operations shall be provided by the NIMS Agent.

3.2.1.3.5 Frequency of transmission

- a) The NIMS Agent shall send SNMP Trap messages to the NIMS Manager upon the occurrence of events.
- b) The NIMS Manager shall send SNMP GetRequest messages to the NIMS Agent at a frequency agreed upon by the FAA to receive status information from the NAS Subsystem.
- c) The NIMS Manager shall send SNMP SetRequest messages to the NIMS Agent as required to control the NAS subsystem.

3.2.1.4 Interface summary table

- a) A summary of the messages to be exchanged across the interface is provided in Table 3-4. This interface shall provide the availability to transfer the listed messages between application processes.

3.2.1.5 Quality of service

3.2.1.5.1 Information priority

- a) Management information shall be communicated as the highest priority data in accordance with FAA-STD-043 when traversing FAA interfacility communications networks (e.g., NADIN PSN).

3.2.1.5.2 Information security

- a) Data access control shall be provided in accordance with the Definition of Administrative Relationships defined in RFC 1157.
- b) Data-origin authentication shall be provided in accordance with the Definition of Administrative Relationships defined in RFC 1157.

3.2.1.6 Error handling

- a) The NIMS Manager and NIMS Agent shall report errors received from PDU operations to the application process.

Table 3-4. Interface Summary Table

A NIMS Manager	B Message	SNMPv1	Direction	C NIMS Agent
Event Reporting Service	Subsystem Status Change	Trap	A<-C	Event Reporting Service
	Subsystem Function Status Change	Trap	A<-C	
	Software Component Status Change	Trap	A<-C	
	Hardware Component Status Change	Trap	A<-C	
	External Interface Status Change	Trap	A<-C	
	Administrative State Change	Trap	A<-C	
	Logical Configuration Change	Trap	A<-C	
	Physical Configuration Change	Trap	A<-C	
	Workload Threshold Transition	Trap	A<-C	
	Throughput Threshold Transition	Trap	A<-C	
	Response Time Threshold Transition	Trap	A<-C	
	Access Control Rule Violation	Trap	A<-C	
Solicited Data Report Service	Report Monitored Attribute	GetRequest	A->C	Solicited Data Report Service
	Monitored Attributes	GetResponse	A<-C	
	Report Control Attributes	GetRequest	A->C	
	Control Attributes	GetResponse	A<-C	
Control Service-Action	Reset Subsystem	GetRequest	A->C	Control Service-Action
	Confirmation	GetResponse	A<-C	
	Perform Diagnostics	GetRequest	A->C	
	Confirmation	GetResponse	A<-C	
Control Service - Modify	Automatic Fault Isolation Parameters	SetRequest	A->C	Control Service - Modify
	Confirmation	GetResponse	A<-C	
	Fault Recovery Processing	SetRequest	A->C	
	Parameters			
	Confirmation	GetResponse	A<-C	
	Event Forwarding Discriminators	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Fault Management Threshold	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Administrative State	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Change Logical Configuration	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Change Physical Configuration	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Performance Thresholds	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	
	Access Control Rules	SetRequest	A->C	
	Confirmation	GetResponse	A<-C	

b) SNMPv1 errors shall include the following in accordance with RFC 1157:

- PDU too large
- No such name
- Bad value
- Read only
- General error

3.2.2 Communication requirements

3.2.2.1 Application layer

- a) The Simple Network Management Protocol Version 1 (SNMPv1) shall be implemented in accordance with RFC 1157.
- b) The File Transfer Protocol shall be implemented in accordance with RFC 959.

3.2.2.2 Presentation layer

This section is not applicable to this ICD.

3.2.2.3 Session layer

This section is not applicable to this ICD.

3.2.2.4 Transport layer

- a) The user Datagram Protocol (UDP) shall be implemented in accordance with RFC 768.
- b) The Transmission Control Protocol (TCP), which will be used with FTP, shall be implemented in accordance with RFC 793.

3.2.2.5 Network layer

- a) The Internet Protocol (IP) shall be implemented in accordance with RFC 791.
- b) The Internet Control Management Protocol (ICMP) shall be implemented in accordance with RFC 792.

3.2.2.6 Addressing

- a) IP addressing shall be in accordance with the FAA Enterprise Network Naming and Addressing Standard: ENET1370-001.1 or its latest revision.

3.2.2.7 Subnetwork profile 1: point-to-point interface

Network Layer

- a) The Internet Protocol Control Protocol (IPCP) shall be implemented in accordance with RFC 1332.
- b) IP datagram shall be mapped to RFC 1661 in accordance with RFC 1332.

Data Link Layer

- c) The Point-to-Point Protocol (PPP) shall be implemented in accordance with RFC 1661.

Physical Layer

Electrical characteristics

- d) For low speed, an unbalanced EIA/TIA-232E shall be supported as defined in FAA-STD-039.
- e) For high speed, a balanced EIA-530 shall be supported as defined in FAA-STD-039.
- f) Full duplex shall be supported.
- g) Clocking shall be provided in a direct connectivity.
- h) Null modem cable shall be used if no modem is used in a direct connectivity.

Data rate

- i) Line speeds shall be supported in accordance with EIA-530 and EIA/TIA-232E as defined in FAA-STD-039.

Cable length

- j) Cable lengths for unbalanced low speed lines shall be in accordance with EIA/TIA-232.
- k) Cable lengths for balanced low speed lines shall be in accordance with EIA-530.
- l) Cable lengths for balanced high speed lines shall be in accordance with EIA-530.

Mechanical characteristics

- m) D-shaped, 25-pin interface connectors shall be used for all interchange circuits in accordance with ISO 2110.
- n) The data terminal equipment (DTE) shall require male (pin) contacts and a female shell (plug connector).
- o) The data circuit-terminating equipment (DCE) shall require female contacts and a male shell.

Functional characteristics

- p) Pin assignments for interface functions shall be in accordance with EIA/TIA-232 and EIA-530.

3.2.2.7.1 Dedicated connection

- a) The NIMS Agent shall be responsible for initiating the connection when dedicated communication services are used.
- b) Under dedicated connection circumstances, the NIMS Agent and the NIMS Manager shall maintain continuous connection.
- c) In the event of disconnection, e.g., due to Managed System or NIMS Manager internal processing such as shut down, restart, communication loss, etc., the NIMS Agent shall initiate a connection establishment procedure.

3.2.2.7.2 Dial-up connection

- a) The NIMS Manager and the NIMS Agent shall be able to establish a connection with the NIMS Agent over a dial-up telephone line.
- b) When called over its dial up connection, the called party shall authenticate the calling party in accordance with approved access control and authentication mechanism.
- c) The originator of the call shall be capable of terminating the connection after an operationally specified period of inactivity on the circuit.

3.2.2.8 Subnetwork profile 2: local area network interface

Local area network (LAN) interfaces shall be in accordance with NAS-IR-4001000: NAS LAN/User Systems Interface Requirements Document and FAA-HDBK-002.

3.2.2.9 Subnetwork profile 3: packet switching interface

Packet switching interfaces shall be in accordance with NAS-IC-43020001: NADIN PSN X.25/Packet Mode User Interface Requirements Document and FAA-HDBK-002.

3.3 Security

Security requirements shall be in accordance with applicable requirements in FAA-STD-045: OSI Security Architecture, Protocol and Mechanisms or its revision.

4. QUALITY ASSURANCE PROVISIONS

4.1 General

Verification shall be in accordance with Table 4-1, Verification Requirements Traceability Matrix (VRTM). The verification levels and methods used in this ICD are presented below.

4.2 Special verification levels and methods

There are no special verification requirements imposed by this ICD.

4.3 Verification levels and methods

- a) There are three basic levels of verification. All requirements imposed by section 3 of the ICD shall be verified at one or more of the following three levels:
- b) Subsystem Level. This level of verification is usually accomplished by the subsystem's contractor testing with the FAA test support operating the interfacing subsystem during testing. The contractor will determine in the test planning documentation the allocation (factory, site) of the test requirements identified in the VRTM. The contractor's completion of validating all elements within the VRTM culminates in the formal qualification of the interface end-item.
- c) Integration Level. This level of verification is conducted by the FAA after interface qualification and acceptance testing by the contractor and during Operational Test and Evaluation (OT&E)/Integration testing. This testing is also identified as FAA end-to-end testing. The OT&E/Integration test plan will determine the location for testing, e.g., FAA Technical Center test site.
- d) Site Level. This level of verification is usually performed at the designated site. The verification portion of the subsystem installation and checkout will emphasize the demonstration of the overall system, the final acceptance demonstrations, and commissioning activities. All verification levels for subsystem to facilities interface would normally occur at the installation site.

4.4 Quality conformance inspections

The VRTM presented in Table 4-1 lists the requirements to be verified, the phase or levels at which verification will occur, and the method of verification that will be used.

4.5 Verification requirements

Compliance with the requirements stated in the ICD are deemed met when all the requirements specified in a paragraph are verified by one or more of the methods outlined in the subsequent subparagraphs. The results of the verification activities shall be expressed as either pass or fail.

4.6 Verification methods

There are four verification methods that can be used at any of the three verification levels. Verification methods are:

- a) Analysis. This method of verification consists of comparing hardware or software design with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements. When certain elements of design are comprised of previously qualified elements such as commercial off the shelf (COTS) equipment, then analysis of previous qualification testing in meeting specification requirements may be used to reduce the amount of qualification testing.
- b) Demonstration. Demonstration is a method of verification where qualitative determination of properties is made for configuration items, including software, and/or technical data and documentation measured, in a dynamic state.
- c) Inspection. Inspection is a method of verification to determine compliance without the use of special test equipment, procedures, or services, and consists of a non-destructive static-state examination of the hardware, software, and/or the technical data and documentation.
- d) Test. Test is a method of verification wherein performance is measured during or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance to the success criteria stipulated in the ICD or project specification. The process uses standardized laboratory equipment, procedures, hardware, and/or services.

Table 4-1. Verification Requirements Traceability Matrix

(Verification Methods: D - Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.	INTERFACE REQUIREMENTS				Title
3.1	General Requirements				Title
3.1a	NIMS connectivity	D	D	D	
3.1b	Proxy Agents	D	D	D	
3.2	Functional Requirements				Title
3.2a	NIMS Manager and Agent	D	D	D	
3.2b	IAW section	D	D	D	
3.2.1	Application Process				Title
3.2.1.1	Identification of application process				Title
3.2.1.1a	Manager application process	D-I	D-I	D	
3.2.1.1b	Agent application process	D-I	D-I	D	
3.2.1.2	Type of service required by the AP				Title
3.2.1.2a	Services	D	D	D	
3.2.1.2.1	Event reporting				Title
3.2.1.2.1a	SNMP trap	D-T	D-T	D	
3.2.1.2.1b	Events	D-T	D-T	D	
3.2.1.2.1c	Periodic poll	D-T	D-T	D	
3.2.1.2.1d	Poll response	D-T	D-T	D	
3.2.1.2.1e	Poll invocation and frequency	D	D	D	
3.2.1.2.2	Solicited Data Reporting				Title
3.2.1.2.2a	Request management data	D-T	D-T	D	
3.2.1.2.2b	Type of resource attributes	D-T	D-T	D	
3.2.1.2.2c	SNMP Get Response	D-T	D-T	D	
3.2.1.2.2d	FTP	D-T	D-T	D	
3.2.1.2.3	Control				Title
3.2.1.2.3.1	Initiate actions				Title
3.2.1.2.3.1a	SNMP SetRequest	D-T	D-T	D	
3.2.1.2.3.1b	Actions	D-T	D-T	D	
3.2.1.2.3.1c	SNMP GetResponse	D-T	D-T	D	
3.2.1.2.3.1d	Status action	D-T	D-T	D	
3.2.1.2.3.2	Modify management information				Title
3.2.1.2.3.2a	SNMP SetRequest	D-T	D-T	D	
3.2.1.2.3.2b	Modifiable managed resources	D-T	D-T	D	
3.2.1.2.3.2c	SNMP GetResponse	D-T	D-T	D	
3.2.1.3	Information units				Title
3.2.1.3a	SNMPv1	I	I	X	
3.2.1.3b	Echo Protocol	D-T	D-T	D	
3.2.1.3c	FTP	D-T	D-T	D	
3.2.1.3.1	Information code				Title
3.2.1.3.1a	Abstract syntax	I	I	X	
3.2.1.3.1b	Transfer syntax	D-T	D-T	X	
3.2.1.3.1.1	Protocol data unit				Title
3.2.1.3.1.1a	SNMPv1	D-I	D-I	X	

Table 4-1. Verification Requirements Traceability Matrix (Continued)

(Verification Methods: D - Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.2.1.3.2	Information structure				Title
3.2.1.3.2a	MIB-II	I	I	X	
3.2.1.3.2b	Private MIB extension	I	I	X	
3.2.1.3.2c	MIB-II object group	I	I	X	
3.2.1.3.2d	Transmission group	I	I	X	
3.2.1.3.2e	Object naming	I	I	X	
3.2.1.3.2.1	NIMS MIB Structure				Title
3.2.1.3.2.1a	NIMS Manager and NIMS Agent	I	I	X	
3.2.1.3.2.1b	NIMS MIB OID name	I	I	X	
3.2.1.3.2.1c	NIMS MIB OID number	I	I	X	
3.2.1.3.2.1d	NIMS MIB standard	I	I	X	
3.2.1.3.2.1e	Specific resources group arc	I	I	X	
3.2.1.3.2.1f	Common resources group	I	I	X	
3.2.1.3.2.1g	Specific resources group availability status	I	I	X	
3.2.1.3.2.1h	Unique resource identifier	I	I	X	
3.2.1.3.2.1i	Managing multiple subsystem	D-T	D-T	D	
3.2.1.3.2.1j	Agent resources	I	I	X	
3.2.1.3.2.2	NIMS Standard Traps	I	I	X	
3.2.1.3.2.2.1	Operating status change				Title
3.2.1.3.2.2.1a	Trap	D-T	D-T	D	
3.2.1.3.2.2.1b	Variable bindings	D-T	D-T	D	
3.2.1.3.2.3	Manage subsystem specific Traps	I	I	X	
3.2.1.3.2.3.1	Availability status change				Title
3.2.1.3.2.3.1a	Trap	D-T	D-T	D	
3.2.1.3.2.3.1b	Variable binding	D-T	D-T	D	
3.2.1.3.2.3.2	Configuration change				Title
3.2.1.3.2.3.2a	Trap	D-T	D-T	D	
3.2.1.3.2.3.2b	Unique name	D-T	D-T	D	
3.2.1.3.2.3.2c	Unique Trap	D-T	D-T	D	
3.2.1.3.2.3.2d	Variable binding	D-T	D-T	D	
3.2.1.3.2.3.3	Performance threshold transition				Title
3.2.1.3.2.3.3a	Trap	D-T	D-T	D	
3.2.1.3.2.3.3b	Unique name	D-T	D-T	D	
3.2.1.3.2.3.3c	Unique Trap	D-T	D-T	D	
3.2.1.3.2.3.3d	Variable binding	D-T	D-T	D	
3.2.1.3.2.3.4	Security violation				Title
3.2.1.3.2.3.4a	Trap	D-T	D-T	D	
3.2.1.3.2.3.4b	Unique name	D-T	D-T	D	
3.2.1.3.2.3.4c	Unique Trap	D-T	D-T	D	
3.2.1.3.2.3.4d	Variable binding	D-T	D-T	D	
3.2.1.3.2.3.5	Shut down complete				Title
3.2.1.3.2.3.5a	Trap	D-T	D-T	D	
3.2.1.3.2.3.5b	Variable binding	D-T	D-T	D	

Table 4-1. Verification Requirements Traceability Matrix (Continued)

(Verification Methods: D - Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.2.1.3.3	Information unit segmentation				Title
3.2.1.3.3a	Size	D-T	D-T	X	
3.2.1.3.4	Information flow				Title
3.2.1.3.4a	IAW Table 3-1	D-T	D-T	D	
3.2.1.3.4b	Event reports	D-T	D-T	D	
3.2.1.3.4c	Solicited data requests	D-T	D-T	D	
3.2.1.3.4d	Solicited data response	D-T	D-T	D	
3.2.1.3.4e	Control operation request	D-T	D-T	D	
3.2.1.3.4f	Control operation completion	D-T	D-T	D	
3.2.1.3.5	Frequency of transmission				Title
3.2.1.3.5a	SNMP Traps	D-T	D-T	D	
3.2.1.3.5b	SNMP GetRequest	D-T	D-T	D	
3.2.1.3.5c	SNMP SetRequest	D-T	D-T	D	
3.2.1.4	Interface summary table				Title
3.2.1.4a	Message exchange	D-T	D-T	D	
3.2.1.5	Quality of service				Title
3.2.1.5.1	Information priority				Title
3.2.1.5.1a	Management information	D-T	D-T	D	
3.2.1.5.2	Information security				Title
3.2.1.5.2a	Access control	D-T	D-T	D	
3.2.1.5.2b	Authentication	D-T	D-T	D	
3.2.1.5.6	Error handling				Title
3.2.1.5.6a	Manager and agent	D-T	D-T	D	
3.2.1.5.6b	SNMP errors	D-T	D-T	D	
3.2.2	Communication requirements				Title
3.2.2.1	Application layer				Title
3.2.2.1a	Management protocol	D	D	D	
3.2.2.1b	Loop-back testing protocol	D-T	D-T	D	
3.2.2.1c	File Transfer Protocol	D-T	D-T	D	
3.2.2.2	Presentation layer	X	X	X	Title
3.2.2.3	Session layer	X	X	X	Title
3.2.2.4	Transport layer				Title
3.2.2.4a	User datagram protocol	D-T	D-T	X	
3.2.2.4b	Transmission Control Protocol	D-T	D-T	X	
3.2.2.5	Network Layer				Title
3.2.2.5a	Internet protocol	D-T	D-T	X	
3.2.2.5b	Internet Control Management Protocol	D-T	D-T	X	
3.2.2.5c	End System to Intermediate System	D-T	D-T	X	
3.2.2.6	Addressing				Title
3.2.2.6a	Addressing protocol	D-T	D-T	X	
3.2.2.7	Subnetwork Profile 1: Point-to-Point Interface				Title
3.2.2.7a	IPCP	D-T	D-T	X	
3.2.2.7b	IP datagrams	D-T	D-T	X	

Table 4-1. Verification Requirements Traceability Matrix (Continued)

(Verification Methods: D - Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.2.2.7c	PPP	D-T	D-T		
3.2.2.7d	Low speed	D-T	D-T	D	
3.2.2.7e	High speed	D-T	D-T	D	
3.2.2.7f	Full duplex	D-T	D-T	D	
3.2.2.7g	Clocking	D-T	D-T	D	
3.2.2.7h	Null modem	D-T	D	D	
3.2.2.7i	Line speed	D-T	D-T	D	
3.2.2.7j	Unbalance low speed lines cable length	D-T	D-T	D	
3.2.2.7l	Balance low speed lines cable length	D-T	D-T	D	
3.2.2.7m	High speed lines cable length	D-T	D-T	D	
3.2.2.7n	Connectors	I	I	X	
3.2.2.7o	DTE	I	I	X	
3.2.2.7p	DCE	I	I	X	
3.2.2.7.1	Dedicated connection				Title
3.2.2.7.1a	Initiating connection	D-T	D-T	D	
3.2.2.7.1b	continuous connection	D-T	D-T	D	
3.2.2.7.1c	Disconnection	D-T	D-T	D	
3.2.2.7.2	Dial-up connection				Title
3.2.2.7.2a	Establish Connection	D-T	D-T	D	
3.2.2.7.2b	Authentication	D-T	D-T	D	
3.2.2.7.2c	Terminating connection	D-T	D-T	D	
3.2.2.8	Subnetwork profile 2	D-T	D-T	D	
3.2.2.9	Subnetwork profile 3	D-T	D-T	D	
3.3	Security requirements	D-T	D-T	D	

5. PREPARATION FOR DELIVERY

This section is not applicable to this ICD.

6. NOTES

6.1 Operational concept

The purpose of this section is to identify the mission requirements pertinent to this interface and to provide an operational description of information interchange between the NAS Subsystem and the NIMS Manager.

6.1.1 NAS Infrastructure Management (NIM) operational concept

Safe operation of the National Airspace System (NAS) depends on high availability and reliable performance of equipment and software. The operating philosophy of NIM is based upon managing the NAS infrastructure so that required services are provided to customers based on established performance standards, customer expectations and business objects.

6.1.1.1 NIM element mission requirements

The NIM element consists of four sub-elements: the NAS Infrastructure Management System (NIMS), National Operations Control Center (NOCC), Operations Control Center (OCC), and Work Centers (WC).

6.1.1.1.1 NIMS sub-element mission requirements

The mission of NIMS is to provide remote performance monitoring and management of NAS infrastructure (systems, subsystems, and equipment and the services it provides). NIMS consists of two major components, managers and agents. The NIMS Manager will manage NAS subsystems remotely through NIMS Agents which monitor management data provided by the NAS subsystem. NIMS Managers will reside in the OCCs and NOCC, but may also reside in the WC in the future.

It is also the mission of the system to provide NIMS users with automated access to the management information collected by the NIMS Manager.

6.1.1.1.2 National Operations Control Center (NOCC)

The NOCC is the organizational entity responsible for determining the overall status of the NAS on a continuous basis and implementing national operations priorities to ensure the smooth functioning of the NAS infrastructure. Specialists will utilize NIMS to monitor the NAS status from a national perspective and develop national and regional infrastructure strategies for short and long term planning purposes.

6.1.1.1.3 Operations Control Center (OCC)

The OCC is the organizational entity responsible for monitoring, managing, and maintaining services and equipment that are specific to the facility's area of responsibility. The OCC, which will provide centralized management of the NAS infrastructure, is the result of the FAA transition from the decentralized Maintenance Control Center concept to the centralized Prototype OCC concept.

The OCC will coordinate with the WC, adjacent OCCs, and the NOCC to implement national priorities. Specialists within the OCC will utilize NIMS to monitor and manage the NAS infrastructure from an area perspective and develop infrastructure strategies for short and long term planning purposes.

6.1.1.1.4 Work Center (WC)

The WC is the organizational entity responsible for working with their respective area OCC to maintain the infrastructure within their facility's area of responsibility. Where the system or facilities cannot be restored remotely, personnel from the WCs will travel to the site and perform necessary maintenance action to restore the system or facility to normal operation.

6.2 Definitions

Administrative State - An attribute which indicates whether or not a managed resource is "unlocked" or "locked" to provide its intended service or in the process of shutting down. This state is set by the NIMS Manager to effect or reflect the status of the managed resource.

Agent - Entity capable of performing management operations on managed resources and emitting notifications on behalf of managed resources.

Attribute - A property of a managed resource.

Availability Status - A monitored attribute that provides more specific information on the condition of the managed resource allocated to provide service. The availability status for the "available" and "not available" administrative states includes the following:

- Available
- On-line
- Power on
- Not Available
- Off-line
- Power on
- Maintenance
- Failed

Degraded - The managed resource is not operating in the ideal range but operating within an acceptable range.

Failed - The managed resource is operating outside the acceptable operating range.

Locked - The value of the Administrative State that is used by the NIMS Manager to prohibit the managed resource from performing its functions for its users. This is equivalent to the NOT AVAILABLE state in NIMS as defined in the NIMS System Level Specification (SLS).

Manager - Entity capable of issuing management operations and receiving notifications.

Managed resource - Resources that may be managed through the use of management protocols.

Normal - The managed resource is operating within the ideal operating range.

Operating Status - Operating status is a monitored attribute, which indicates to the extent to which a subsystem resource can perform its intended operation. Operating status is resource dependent and the specific characterization varies with the operating range of the resource. Four indicators are provided to characterize the operational status of a resource: normal, warning, degraded, and failed.

Proxy agent - Entity capable of providing interface conversion with a non-standard agent to perform management operations on managed objects and emit notifications on behalf of managed objects.

Shutting Down - The value of the Administrative State that is used by the NIMS Manager to direct the managed resource to begin gracefully making itself unavailable to perform its functions for its users.

Unlocked - The value of the Administrative State that is used by the NIMS Manager to permit the managed resource to perform its functions for its users. This is equivalent to the AVAILABLE state in NIMS as defined in the NIMS SLS.

Warning - The managed resource is still capable of performing all of its functions at the ideal level of performance, but some aspect of the resource has changed such that management action is required.

6.3 Abbreviations and acronyms

AP	Application Process
BER	Basic Encoding Rules
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CCITT	International Telegraph and Telephone Consultative Committee
COTS	Commercial-off-the-shelf

CRG	Common Resources Group
ICD	Interface control document
DCE	Data circuit-terminating equipment
DOD	Department of Defense
DTE	Data terminal equipment
EIA	Electronic Industries Association
ES	End system
FAA	Federal Aviation Administration
FDDI	Fiber Data Distributed Data Interface
FTP	File Transfer Protocol
ICD	Interface Control Document
ICMP	Internet Control Message Protocol
IEC	Engineering Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPS	Internet Protocol Suite
IPT	Integrated Product Team
IRD	Interface Control Documents
IS	Intermediate System
ISO	International Organization for Standardization
LAN	Local area network
LAPB	Link Access Protocol - Balanced
MCC	Maintenance Control Center
MIB	management information base
Mgmt	Management
NADIN	National Data Interchange Network
NAS	National Airspace System
NIMS	NAS Infrastructure Management System
NOCC	National Operations Control Center
OCC	Operations Control Center
OID	Object Identifier
ORD	Operational requirements document
OT&E	Operational test and evaluation
PDU	Protocol data unit
PPP	Protocol-to-Point Protocol
PSN	Packet switching network
PT	Product Team
RFC	Request for Comments
SLS	System Level Specification

SNMP	Simple Network Management Protocol
SRG	Specific Resources Group
SSC	Service Support Center
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VRTM	Verification Requirements Traceability Matrix
WAN	Wide area network
WC	Work Center

APPENDIX A

SMI DEFINITIONS OF SNMPv1 CONSTRUCTS FOR FAA NIMS

A.1 FAA NIMS MIB

MIBfaaNimsSNMPv1 DEFINITIONS ::= BEGIN

IMPORTS

enterprises, TimeTicks
FROM RFC1155-SMI
OBJECT-TYPE
FROM RFC-1212
Display String
FROM RFC1213-MIB;

FaaEnterprise OBJECT IDENTIFIER ::= {enterprises 2120}
nims OBJECT IDENTIFIER ::= {faaEnterprise 1}
commonResourcesGroup OBJECT IDENTIFIER ::= {nims 1}
specificResourcesGroup OBJECT IDENTIFIER ::= {nims 2}

-- the Common Resource Group table

crgNumber OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Number of Entries in crgTable."
::= {commonResourcesGroup 1}

crgTable OBJECT-TYPE
SYNTAX SEQUENCE OF CrgTableEntry
ACCESS not-accessible
STATUS mandatory
DESCRIPTION
"Table of common managed resource attributes."
::= {commonResourcesGroup 2}

crgTableEntry OBJECT-TYPE
SYNTAX CrgTableEntry
ACCESS not-accessible
STATUS mandatory

DESCRIPTION

“Defines the conceptual row for crgTable.”

INDEX {crgID}

::= {crgTable 1}

CrgTableEntry ::= SEQUENCE {crgID	DisplayString,
crgDescr	DisplayString,
crgType	INTEGER,
crgOpStatus	INTEGER,
crgAdminState	INTEGER,
crgOpTime	TimeTicks,
crgSrgOID	OBJECT IDENTIFIER}

crgID OBJECT-TYPE

SYNTAX DisplayString (SIZE (0..20))

ACCESS read-only

STATUS mandatory

DESCRIPTION

“Resource unique identifier of managed resource component.”

::= {crgTableEntry 1}

crgDescr OBJECT-TYPE

SYNTAX DisplayString (SIZE (0..50))

ACCESS read-only

STATUS mandatory

DESCRIPTION

“Information about the managed resource component.”

::= {crgTableEntry 2}

crgType OBJECT-TYPE

SYNTAX INTEGER { subSystem (1),
subFunction (2),
hwComponent (3),
swComponent (4),
extInterface (5),
agentFunction (6)}

ACCESS read-only

STATUS mandatory

DESCRIPTION

“Type of managed resource component - (1) subsystem, (2) subsystem function, (3) hardware component, (4) software component, (5) external subsystem interface (6) agent function.”

::= {crgTableEntry 3}

crgOpStatus OBJECT-TYPE

SYNTAX INTEGER { normal (1),
warning (2),
degraded (3),
fail (4)}

ACCESS read-only

STATUS mandatory

DESCRIPTION

“Operating status of managed resource component - (1) normal, (2) warning, (4) degraded, (4) failed.”

::= {crgTableEntry 4}

crgAdminState OBJECT-TYPE

SYNTAX INTEGER {locked (1),
unlocked (2),
shuttingDown (3)}

ACCESS read-write

STATUS mandatory

DESCRIPTION

“Administrative state of managed resource component - (1) locked, (2) unlocked, (3) shutting down.

If the resource cannot have its Administrative State changed remotely, the Administrative State will be permanently set to “unlocked”, and when a Set-Request is received to SET the value to “locked” or “shuttingDown”, the resultant Get-Response shall be returned with a value of “unlocked”. If the resource does support the shuttingDown state, the resource shall generate a managed subsystem-specific trap whenever the value of the Administrative State transitions from “shuttingDown” to “locked”.”

If the resource does not support the “shutting down” state, when a Set-request is received to SET the value to “shuttingDown”, the resource shall immediately transition to “locked” and the resultant Get-Response shall be returned with a value of “locked”.

::= {crgTableEntry 5}

crgOpTime OBJECT-TYPE

SYNTAX TimeTicks

ACCESS read-only

STATUS mandatory

DESCRIPTION

“Value of system time when the managed resource entered its current status or state.”

::= {crgTableEntry 6}

crgSrgOID OBJECT-TYPE

SYNTAX OBJECT IDENTIFIER
ACCESS read-only
STATUS mandatory
DESCRIPTION

“OID of the Specific Resources Group table that contains additional
management information about the resource.”
::= {crgTableEntry 7}

END

A.2 NIMS-Standard Traps

A.2.1 opStatusChange Trap

opStatusChange TRAP-TYPE
ENTERPRISE faaEnterprise
VARIABLES {crgOpStatus}
DESCRIPTION

“Trap caused by change in the
operating status attribute of the
managed resource. The operating
status attribute ‘crgOpStatus’
indicates one of four conditions:
NORMAL (1) - resource is operating
in the ideal operating range;
WARNING (2) - resource is still
capable of performing all of its
functions at the ideal level of
performance, but some aspect of the
resource has changed such that
management action is required;
DEGRADED (3) - resource not
operating in the ideal operating range
but operating within an acceptable
operating range; or FAILED (4) -
resource operating outside the
acceptable operating range.”

::=1